UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/649,804	08/26/2003	Iven Connary	600323-086	6001

61834 7590 11/16/2007

DREIER LLP
499 PARK AVE
NEW YORK, NY 10022

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
11/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/649,804	CONNARY ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 11/30/2006.Claims 1, 5,8,-13 have been amended. Claims 1-13 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

3. The examiner does not withdraws the 35 USC 101 rejection because "calculating a differential treat level, calculating a compound host threat, determining a host treat level, determine a destination vulnerability, determine a source threat and determine an event severity" do not produce a tangible result.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 5-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al (hereinafter referred as Farley) US Patent 7,089,428 B2 in view of O'Sullivan(US Pub No 2006/0095569 A1).**

6. As per claim 5: Farley disclose a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61

through col 10 line 28); and based upon the event data (Fig 5b step 505); determining a host threat level (See col 12 line 30 through col 13 line 20).

Farley does not explicitly teach determining a host threat level based upon a treat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member.

However O'Sullivan teaches determining a host threat level based upon a treat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member (See 0028-0029,0089-0091 and Fig 11).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system.

7. As per claim 6: the combination of Farley and OSulivan teach a method wherein the host is a source device (See Farley Fig 5D step 503 and Fig 5F step 513).

8. As per claim 7: the combination of Farley and OSulivan teach wherein the host is a destination device (See Farley Fig 5F step 513).

9. As per claim 8: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data (See Fig 5B and See col 12 line 30 through col 13 line 20); and determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host

network block of which the host is a member(See Fig 5F step 513 and See col 12 line 30 through col 13 line 20).

Farley does not explicitly teach determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member (See Fig 5F step 513 and See col 12 line 30 through col 13 line 20).

However O'Sulivan teaches determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member (See 0028-0029, 0043, 0089-0091 and Fig 11).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system.

10. As per claim 9: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28)

Farley does not explicitly teach determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member(See Fig 5F step 513 and col 19 lines 10-

46); determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type.

However O'Sulivan teaches determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member(See 0028-0029, 0043, 0089-0091 and Fig 11); determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host(See 0028-0029, 0043, 0089-0091 and Fig 11)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system.

11. As per claim 10: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46);determining an event validity based upon the source and the event type(See col 15 lines 24-38,col 17

lines 33-46 and col 19 lines 10-46); and determining an event severity base upon the event type(See Fig 5Bstep 555 and col 10 lines 29-34); and calculating the network security threat based upon the source threat, the destination vulnerability, the event validity, and the event severity(See col 23 line 61 through col 24 line 46 and Fig 7).

Farley does not explicitly teach determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member; determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.

However O'Sulivan teaches determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member (0028-0029, 0043, 0089-0091 and Fig 11);determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member(See 0028-0029, 0043, 0089-0091 and Fig 11).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system.

12. As per claim 11: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data(See Fig 5Bstep 555 and col 10 lines 29-34); determining a destination vulnerability by associating the destination threat value with a destination vulnerability value eased upon a vulnerability of a destination host for the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining an event validity based upon the source and the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); and determining an event severity base upon the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); calculating an event threat based upon the source threat, the destination vulnerability, the event validity, and the event severity(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); calculating a compound host threat by associating a plurality of event threats over a time period with a number of correlated events in the time period(See col 15 lines 24-38,col 24 lines 1-39).

Farley does not explicitly teach determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member;determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block

threat weighting for the event type assigned to a host network block of which the host is a member.

However O'Sulivan teaches determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member (0028-0029, 0043, 0089-0091 and Fig 11);determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member(See 0028-0029, 0043, 0089-0091 and Fig 11).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system.

13. As per claim 12: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data (See Fig 5Bstep 555 and col 10 lines 29-34); determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining an event validity based upon the source and the event type(See Fig 5Bstep 555 and col 10 lines 29-34); and determining

an event severity base upon the event type(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining an event threat based upon the source threat, the destination vulnerability, the event validity, and the event severity(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining a first compound host threat value by associating a first plurality of event threats over a first time period with a first frequency number of correlated events in the first time period(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining a second compound host threat value by associating a second plurality of event threats over a second time period greater than the first time period with a second frequency number of correlated events in the second time period; and determining a differential threat level by associating the first compound host threat value with the second host threat value(See col 15 lines 24-38,col 24 lines 1-39)

Farley does not explicitly teach determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member; determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.

However O'Sulivan teaches determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is

a member (0028-0029, 0043, 0089-0091 and Fig 11);determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member(See 0028-0029, 0043, 0089-0091 and Fig 11).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley method inorder to enhance security of the system

13. Claims 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al (hereinafter referred as Farley) US Patent 7,089,428 B2 in view of Mcclure et al(hereinafter referred as Mcclure) US patent no 7152105 B2 and further view of O'Sullivan(US Pub No 2006/0095569 A1).

14. As per claims 1: Farley discloses a computer-implemented method for determining network security threat level, comprising the steps of: receiving event data in response to identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); based upon the event data, perform the following step: determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member (See Fig 5F step 513 and See col 12 line 30 through col 13 line 20); determining a destination vulnerability value, the destination vulnerability value based upon the network event in conjunction with a destination IP address, a destination threat weight for the destination IP address,

and a threat level value associated with a second range of network IP address of which the destination IP address is a member(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46); determining an event validity value based upon the source IP address and an event type determining event severity value based upon the event type(See col 23 line 61 through col 24 line 46 and Fig 7); calculating an event threat level value based upon the source threat value, the destination vulnerability value, the event validity value, and the event severity value(See col 23 line 61 through col 24 line 46 and Fig 7);

Farley does not explicitly disclose calculating a host threat level value based upon a summation of event threat level values for a host over a first time period associated with a number of correlated events for the host in the first time period; and calculating a differential threat level by associating the host threat level value with a second host threat level value based upon a second time period wherein the second time period exceeds the first time period.

However Mcclure teach calculating a host threat level value based upon a summation of event threat level values for a host over a first time period associated with a number of correlated events for the host in the first time period (See col 9 line 17 through col 10 line 28); and calculating a differential threat level by associating the host threat level value with a second host threat level value based upon a second time period wherein the second time period exceeds the first time period (See col 9 line 17 through col 10 line 28).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Mcclure within Farley method inorder to provides a computer security management system that can log, investigate, respond to, and track computer security incidents that can occur in networked computer system (See Mcclure col 3 lines 25-29).

The combination of Farley and Mcclure do not explicitly teach determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member (See Fig 5F step 513 and See col 12 line 30 through col 13 line 20); determining a destination vulnerability value, the destination vulnerability value based upon the network event in conjunction with a destination IP address, a destination threat weight for the destination IP address, and a threat level value associated with a second range of network IP address of which the destination IP address is a member(See col 15 lines 24-38,col 17 lines 33-46 and col 19 lines 10-46);

However O'Sullivan teach determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member(See 0028-0029, 0043, 0089-0091 and Fig 11)); determining a destination vulnerability value, the destination vulnerability value based upon the network event in conjunction with a destination IP address, a destination threat weight for the destination IP address, and a threat level value associated with a second range of network IP address of which the destination IP address is a member(See 0028-0029, 0043, 0089-0091 and Fig 11);

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of O'Sulivan within Farley-Mcclure method inorder to enhance security of the system

15. **Claims 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al (hereinafter referred as Farley) US Patent 7,089,428 B2 in view of Mcclure et al(hereinafter referred as Mcclure) US patent no 7152105 B2 and further view of Friedrichs et al(hereinafter referred as Friedrichs) US Pub No 2003/0084349.**

14. As per claim 13: Farley discloses a method for determining network security threat level, comprising the steps of: receiving event data in response to an identified network event detected by a sensor (See Fig 5A step 28, Fig 5b step 505 and col 9 line 61 through col 10 line 28); determining an event type based upon the event data (See Fig 5Bstep 555 and col 10 lines 29-34); based upon the event data, perform the following steps:

Farley does not explicitly disclose determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period; determining a second host frequency threat level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period; and determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period; determining a differential threat level denominator by

multiplying the second host frequency value by the first time period, and calculating a differential threat level by diving the differential threat level numerator by the differential threat level denominator.

However Mcclure disclose determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period (See col 9 line 17 through col 10 line 28); determining a second host frequency threat level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period(See col 9 line 17 through col 10 line 28); determining a differential threat level denominator by multiplying the second host frequency value by the first time period, and calculating a differential threat level by diving the differential threat level numerator by the differential threat level denominator(See col 9 line 17 through col 10 line 28).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Mcclure within Farley method inorder to provides a computer security management system that can log, investigate, respond to, and track computer security incidents that can occur in networked computer system (See Mcclure col 3 lines 25-29).

The combination of Farley and Mcclure do not explicitly teach determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period.

However Friedrichs teaches determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period(See 0037).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Friedrichs within Farley and Mcclure method inorder to enhance security of the system

15. **Claims 2-4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Farley et al (hereinafter referred as Farley) US Patent 7,089,428 B2 in view of O'Sullivan(US Pub No 2006/0095569 A1) and further in view of Mcclure et al(hereinafter referred as Mcclure) US patent no 7152105 B2 and further in view of Black et al(US Patent No 6,928,556 B2).**

16. As per claim 2: the combinations of Farley-Mcclure-O'Sullivan disclose claim 1 as recited above. The combination of Farley-Mcclure-O'Sullivan do not explicitly disclose further comparing the event threat level value to an event alert value; and generating an alarm when the event threat level value exceeds the event alert value.

However Black discloses Black teaches comparing the event threat level value to an event alert value(See Fig 7 steps 704,706); and generating an alarm when the event threat level value exceeds the event alert value(Fig 7 step 708).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Black within the combinations Mcclure-Farley-O'Sullivan method inorder to provides a computer security management

system that can log, investigate, respond to, and track computer security incidents that can occur in networked computer system (See Mcclure col 3 lines 25-29).

17. As per claim 3: the combination of Farley-Mcclure-O'Sullivan teach claim 1 as recited above. The combination of Farley-Mcclure-O'Sullivan do not explicitly disclose further comparing the compound host threat level value t comparing the event threat level value to an event alert value; and generating an alarm when the event threat level value exceeds the event alert value.

However Black teaches comparing the event threat level value to an event alert value (See Fig 7 steps 704,706); and generating an alarm when the event threat level value exceeds the event alert value(Fig 7 step 708).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Black within the combination Mcclure and Farley method inorder to provides a computer security management system that can log, investigate, respond to, and track computer security incidents that can occur in networked computer system (See Mcclure col 3 lines 25-29).

18. As per claim 4: the combination of Farley-Mcclure-O'Sullivan teach claim 1 as recited above. The combination of Farley-Mcclure-O'Sullivan do not explicitly disclose further comparing the differential threat level value to a differential alert value; and generating an alarm when the differential threat level exceeds the differential alert value.

However Black teach comparing the differential threat level value to a differential alert value (See Fig 7 steps 704,706); and generating an alarm when the differential threat level exceeds the differential alert(Fig 7 step 708).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to modify the teaching method of Black within the combination Mcclure-Farley-OSullivan method inorder to provides a computer security management system that can log, investigate, respond to, and track computer security incidents that can occur in networked computer system (See Mcclure col 3 lines 25-29).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser,can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
11/12/07
FA

Art Unit 2136

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER